



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANT'S MAIN BRIEF ON APPEAL

APPELLANT: Kazuo Watanabe OLD DOCKET NO: SONY-U0200
NEW DOCKET NO: 09792909-4910
SERIAL NO.: 09/735,760 GROUP ART UNIT: 2137
DATE FILED: December 13, 2000 EXAMINER: Michael Pyzocha
INVENTION: "METHOD AND APPARATUS FOR MANAGING SOFTWARE
USE"

Mail Stop Appeal Brief - Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Appellant submits herewith Appellant's Main Brief on Appeal under 37 C.F.R. §41.37 in support of the Notice of Appeal mailed on February 15, 2006. The Commissioner is hereby authorized to charge the amount of \$500.00 for the requisite filing fee for filing the Main Brief on Appeal to the Appellants' Attorneys' credit card. Form 2038 is attached.

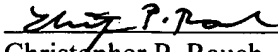
The Commissioner is hereby authorized to charge any deficiency in fees associated with this communication or credit any overpayment to Deposit Account No. 19-3140. A duplicate copy of this sheet is enclosed.

Respectfully Submitted,

Chris P. Rauch (Reg. No. 45,034)
Christopher P. Rauch
SONNENSCHN NATH & ROSENTHAL LLP
P.O. Box #061080
Wacker Drive Station - Sears Tower
Chicago, IL 60606-1080
Telephone 312/876-2606
Customer #26263
Attorneys for Appellants

CERTIFICATE OF MAILING

I hereby certify that correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 17, 2006.

 (Reg. No. 45,034)
Christopher P. Rauch



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANT'S MAIN BRIEF ON APPEAL

APPELLANT:	Kazuo Watanabe	OLD DOCKET NO:	SONY-U0200
		NEW DOCKET NO:	09792909-4910
SERIAL NO.:	09/735,760	GROUP ART UNIT:	2137
DATE FILED:	December 13, 2000	EXAMINER:	Michael Pyzocha
INVENTION:	"METHOD AND APPARATUS FOR MANAGING SOFTWARE USE"		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

In accordance with the provisions of 37 C.F.R. §41.37, Appellant submits this Main Brief on Appeal pursuant to the Notice of Appeal mailed on February 15, 2006 in the above-identified application.

I. REAL PARTY IN INTEREST:

The real party in interest in the present appeal is the Assignee, Sony Corporation. The assignment was recorded in the U.S. Patent and Trademark Office at Reel 011366, Frame 0738.

II. RELATED APPEALS AND INTERFERENCES:

Appellant is not aware of any related appeals or interferences.

III. STATUS OF CLAIMS:

Claims 1-4, 7-10, and 13-14 are pending in the application.

The present appeal is directed to claims 1-4, 7-10, and 13-14, which were finally rejected in an Office Action dated November 15, 2005. A copy of claims 1-4, 7-10, and 13-14 is appended hereto as the Claims Appendix.

The status of the claims on appeal is as follows:

Claims 1-4, 7-10, and 13-14 are rejected under 35 U.S.C. §103(a) as allegedly being

unpatentable over *Olsen* (U.S. Patent No. 5,758,069) (“*Olsen*”) in view of *Uchenick* (U.S. Patent No. 4,458,315) (“*Uchenick*”) and further in view of *Coley, et al.* (U.S. Patent No. 5,790,664) (“*Coley*”).

In the Office Action dated November 15, 2006, the Examiner also finally rejected claim 5, however, claim 5 is currently not pending. (*Office Action of 11/15/2006*, page 2). This appears to be a typographical error.

IV. STATUS OF AMENDMENTS:

All amendments have been entered in this application.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

Claims 1-14 are currently pending. The claimed invention relates to methods and systems for managing the use of software.

Claims 1-6:

Independent claim 1 relates to a method of managing software use by a software provider for distribution to a user. Predetermined first information is stored inside the software. In an illustrative example, the software may include a hash function. (*See, e.g., Figure 3 Hash Function H stored in the software; Specification page 10, lines 1-3*). The software is provided to a software user on an information storage means prepared corresponding to the software and to be connected to an apparatus for running the software. (*Specification, page 4, lines 21-27; page 2, lines 22-28*). The information storage means is capable of being accessed by the apparatus in a connected state. (*Specification, page 2, lines 22-28*).

Second information is encoded by using a first key of a key pair of an open key encoding format. (*Specification page 10, lines 14-20; Figure 6 item 63*). The encoded second information is transmitted to the software user for the software user to decode the transmitted encoded second information by using a second key of the key pair of the open key encoding format, and to read the first information from the information storage means, and to match the read first information

against the decoded second information. (Specification page 10, lines 22-27; Figure 6 item 64).

The software is enabled when the information match. (Specification page 10, line 29-page 11, line 2; Figure 6 items 65 and 66). The encoded second information is transmitted to the software user for matching the read first information against the decoded second information each time the software user uses the software. (Figure 6).

Claims 2-4 depend directly or indirectly from claim 1.

Claims 7-12:

Claim 7 claims subject matter relating to a method of enabling software by a user for software managed by a software provider. Software is received in an information storage means prepared corresponding to the software. (Specification, page 4, lines 21-27; page 2, lines 22-28). Predetermined first information is stored in the software. (See, e.g., Figure 3 Hash Function H stored in the software; Specification page 10, lines 1-3). The information storage means is connected with an apparatus for running the software. The information storage means is capable of being accessed by the apparatus in the connected state. (Specification, page 2, lines 22-28).

Encoded second information is received from the software provider to be matched against the first information stored in the information storage means. The encoding is performed by using a first key of a key pair of an open key encoding format. (Specification page 10, lines 14-20; Figure 6 item 63). The transmitted encoded second information is decoded by using a second key of the key pair of the open key encoding format. The first information is read from the information storage means. (Specification page 10, lines 22-27; Figure 6 item 64). The read first information is matched against the decoded second information. The software is enabled when the information match. (Specification page 10, line 29-page 11, line 2; Figure 6 items 65 and 66). The steps of receiving the encoded second information, decoding the transmitted encoded second information, reading the first information, and matching the read first information against

the decoded second information are performed each time the software user uses the software. (Figure 6).

Claims 8-10 depend directly or indirectly from claim 7.

Claim 13:

Independent claim 13 claims subject matter relating to a system for enabling software stored in an information storage means for accessibly connecting via a predetermined interface means to an apparatus for running the software. The software has first information stored therein. (*See, e.g.*, Figure 3 Hash Function H stored in the software; Specification page 10, lines 1-3). A transmitting means is for transmitting second identification information to a software provider when seeking authorization of use of the stored software. (Figure 6 item 61). A receiving means is for receiving encoded third information transmitted by the software provider to be matched against the first information generated based on the second information. (Specification page 10, lines 14-20; Figure 6 items 63 and 64). The third information is encoded by a first key of a key pair of an open key encoding format. (Specification page 10, lines 14-20; Figure 6 item 63). A decoding means is for decoding the received encoded third information by using a second key of the key pair of the open key encoding format. (Specification page 10, lines 14-20; Figure 6 item 63). A matching means is for matching the first information stored in the information storage means against the decoded third information. (Specification page 10, line 29-page 11, line 2; Figure 6 items 65 and 66). An execution control means is for enabling the software to be used when the information match. (Specification page 10, line 29-page 11, line 2; Figure 6 items 65 and 66). The encoded third information is received for matching against the first information each time a software user uses the software. (Figure 6).

Claim 14:

Claim 14 claims a system for managing software by a software provider. The software is stored in an information storage means to a provider for accessibly connecting via a

predetermined interface means to an apparatus for running the software. (Specification, page 4, lines 21-27; page 2, lines 22-28). The software has first information stored therein. (See, e.g., Figure 3 Hash Function H stored in the software; Specification page 10, lines 1-3). A receiving means is for receiving second identification information from a user seeking authorization of use of the stored software. (Figure 6 item 61). An encoding means is for encoding third information by using a first key of a key pair of an open key encoding format based on the second information. (Specification page 10, lines 14-20; Figure 6 items 63 and 64). A transmitting means is for transmitting the encoded third information to the user to be matched against the first information. (Specification page 10, lines 14-20; Figure 6 item 63). The first information stored in the information storage means is matched against the third information upon being decoded. The software is enabled to be used when the information match. (Specification page 10, line 29-page 11, line 2; Figure 6 items 65 and 66). The encoded third information is transmitted for matching against the first information each time the user uses the software. (Figure 6).

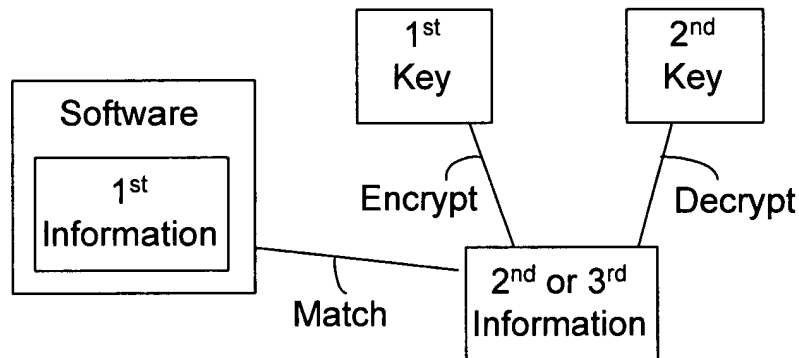
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Claims 1-4, 7-10, and 13-14 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Olsen* (U.S. Patent No. 5,758,069) (“*Olsen*”) in view of *Uchenick* (U.S. Patent No. 4,458,315) (“*Uchenick*”) and further in view of *Coley, et al.* (U.S. Patent No. 5,790,664) (“*Coley*”).

VII. ARGUMENT:

As set forth below, claims 1-4, 7-10, and 13-14 are not unpatentable under 35 U.S.C. §103(a) based on the teachings of *Olsen* in view of *Uchenick* and further in view of *Coley*. Appellant respectfully submits that the Examiner’s assertions are incorrect as a matter of fact and law. Thus, for the reasons set forth below, Appellant respectfully requests that this Board reverse the rejection of claims 1-4, 7-10, and 13-14 under 35 U.S.C. §103(a) as being allegedly unpatentable based on the teachings of *Olsen* in view of *Uchenick* and further in view of *Coley*.

Independent claims 1, 7, 13 and 14 each claim subject matter relating to a software that includes a first information. Each time a user uses the software, an encoded second or third information is transmitted/received for matching against the first information that is stored inside the software. The second or third information is encrypted using a first key and decrypted using a second key. Further, the second or third information is transmitted to a user or from a software provider (e.g., to the user). The software is enabled when the first information and the second or third information match. An illustrative example that depicts these claimed elements is shown below.



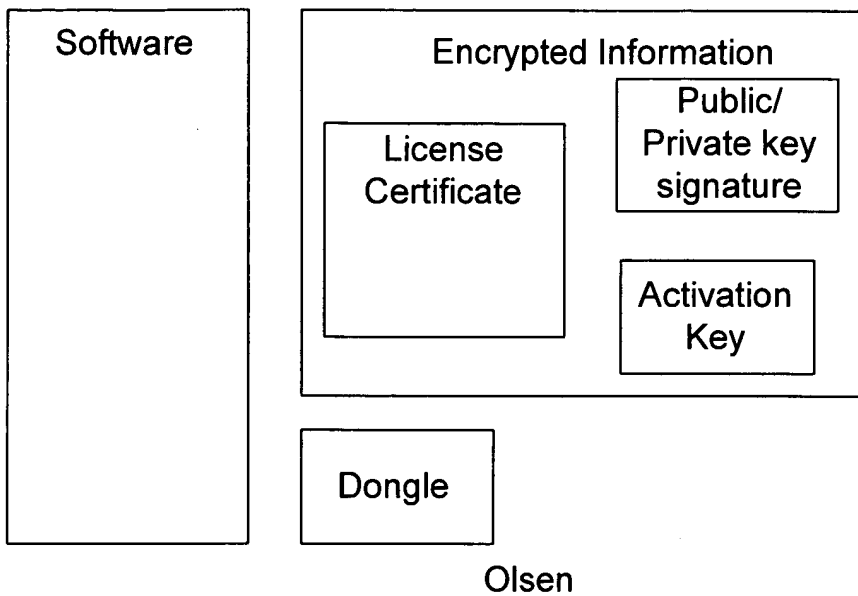
Illustrative example consistent with the claimed invention

This is clearly unlike *Olsen* in view of *Uchenick* and further in view of *Coley*.

A. *Olsen* fails to disclose or suggest the claimed invention

Olsen discloses a system for enabling a software by deploying a license certificate from a database to a software user. In other words, the user can use the software only when the user has received the license certificate. *Olsen* also describes in very brief and abstract terms that the license certificate may be bundled with an activation key and a public/private key signature. *Olsen* 10:12-26. Further, *Olsen* mentions in very brief and abstract terms that its software application may be activated using a hardware security device, such as a “dongle.” *Olsen* 10:26-29. *Olsen*’s dongle is used “to activate the [software] application” and therefore is not used to

validate or activate the license certificate. *Olsen* 10:26-29. *Olsen*'s elements are shown in the figure below.



Olsen fails to discuss how it implements its activation key and public/private key signature. Instead, *Olsen* merely mentions these security devices, but fails to describe what they are and how they are used. For example, *Olsen* mentions that an activation key and public/private key signature may be used, but it is unclear whether these are used to activate the license certificate or the software. *Olsen* calls these security devices “secrets” and states that they “prevent unauthorized *modification of the license certificate*.” *Olsen* 10:20-21 (emphasis added). Therefore, the activation key and public/private key signature apparently are used to validate and activate the license certificate, so that the license certificate may be used to access the software.

What is clear is that *Olsen* does not teach a first information stored in its software. In fact, *Olsen* fails to teach any security-related information stored in its software. Accordingly, *Olsen* could not teach that a first information, which is stored in its software, is matched against a second/third information that has been received.

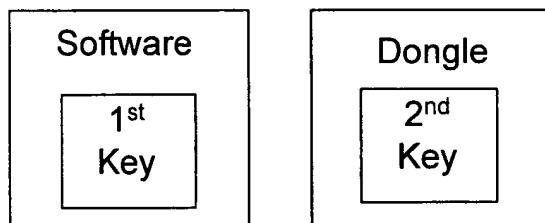
Further, it is clear that *Olsen* fails to disclose or suggest matching a first information to a second information, which is encrypted using a first key and decrypted with a second key. Even

if the Examiner interprets *Olsen's* license certificate to allegedly suggest Appellant's first information, *Olsen's* license certificate is not matched to a second information, let alone a second information that is encrypted with a first key and decrypted with a second key. Even if the Examiner interprets *Olsen's* activation key to allegedly suggest Appellant's second/third information, *Olsen* fails to disclose or suggest that its activation key is encrypted with a first key and decrypted with a second key. Further, *Olsen* does not match its license certificate to its activation key. Instead, *Olsen* merely describes that its activation key may be used to "prevent unauthorized *modification of the license certificate*." *Olsen* 10:20-21 (emphasis added).

Therefore, *Olsen* alone fails to disclose or suggest Appellant's claimed invention.

B. *Olsen* in view of *Uchenick* still fails to disclose or suggest the claimed invention

Uchenick teaches a first key that is included in a software. The first key is compared to a second key that is included in a plug-in device. *Uchenick* Abstract. These components of *Uchenick* are shown in the figure below.



Uchenick

The Examiner argues that *Olsen's* license certificate can be substituted with *Uchenick's* first key and that *Olsen's* activation key can be substituted with *Uchenick's* second key in order to suggest Appellant's claimed first information and second/third information. Appellant respectfully disagrees.

To begin with, *Olsen's* license certificate is a license, not a key that is contained within software. *Olsen* 9:23-63. *Olsen's* license certificate includes information such as product name,

version, number of license units, start date, and end date. *Olsen* 9:23-63. This is clearly not a key that can be matched to another key -- it is a license. *Uchenick*'s first and second keys have a purpose of being matched against each other to enable a software. On the other hand *Olsen*'s license certificate is not something that is matched to something else -- it is merely a license. Therefore, Appellant submits that one having skill in the art would not have been motivated to substitute *Olsen*'s license certificate with *Uchenick*'s first key.

Further, *Olsen*'s activation key cannot be substituted with *Uchenick*'s second key. *Olsen* clearly teaches that its activation key is bundled together with its license certificate in an encrypted information package that is transmitted from a database server. Further, *Olsen* teaches that a hardware dongle is a security device that is different than its activation key. Therefore, Appellant respectfully submits that *Olsen* teaches away from including its activation key in a hardware dongle. Accordingly, Appellant submits that one having skill in the art would not have been motivated to substitute *Olsen*'s electronically-transmitted activation key with *Uchenick*'s second key, which is on a hardware dongle. Accordingly, *Olsen* in view of *Uchenick* fails to disclose or suggest Appellant's claimed second/third information that is matched to Appellant's claimed first information.

Further, *Uchenick* fails to disclose or suggest a second/third information that is encrypted with a first key and decrypted with a second key. Nowhere does *Uchenick* even suggest that its second key is encrypted, let alone encrypted with a first key and decrypted with a second key. As discussed above, *Olsen* also fails to disclose or suggest a second/third information that is encrypted with a first key and decrypted with a second key. Therefore, for at least this additional reason, *Olsen* in view of *Uchenick* fails to disclose or suggest Appellant's claimed invention.

C. *Olsen* in view of *Uchenick* and further in view of *Coley* still fails to disclose or suggest the claimed invention

The Examiner combines *Olsen* and *Uchenick* with *Coley* in an attempt to disclose or suggest transmitting data to be matched each time a software user uses a software. Appellant respectfully submits that, although *Coley* transmits data, *Coley* fails to transmit the data to be matched to a user or from a software provider as claimed. Instead, *Coley* merely sends an inquiry to a licensing system to determine whether the licensing system has a license on record for the user. *Coley* Abstract. Thus, unlike Appellant's claimed invention, *Coley* fails to disclose or suggest transmitting data to a user or transmitting data from a software provider to match against a first information that is in a software. Instead, *Coley* transmits an inquiry to a licensing system to look up a license record in a database.

Further, like *Olsen* and *Uchenick*, *Coley* fails to disclose or suggest matching a first information in a software to a second information, which is encrypted using a first key and decrypted with a second key. Nowhere does *Coley* even mention a software that includes Appellant's claimed first information. Further, as discussed above, *Coley* fails to disclose or suggest a second information that is received at a user or transmitting from a software provider to match against a first information that is in a software.

Further, like *Olsen* and *Uchenick*, *Coley* fails to disclose or suggest a second information that is encrypted using a first key and decrypted with a second key. In fact *Coley* fails to discuss encrypting using a first key and a second key.

Thus, for at least the reasons discussed above, *Olsen* in view of *Uchenick* and further in view of *Coley* fails to disclose or suggest Appellant's independent claims 1, 7, 13, and 14.

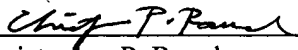
Claims 2-4 and 8-10 depend directly or indirectly from claims 1 or 7 and are therefore allowable for at least the same reasons that claims 1 and 7 are allowable.

Appellants respectfully request that the Board reverse the rejection.

VIII. CONCLUSION:

For the foregoing reasons, Appellants respectfully submit that the rejections posed by the Examiner are improper as a matter of law and fact. Accordingly, Appellants respectfully request the Board reverse the rejections of claims 1-4, 7-10, and 13-14.

Respectfully submitted,

 (Reg. No. 45,034)
Christopher P. Rauch

SONNENSCHN NATH & ROSENTHAL LLP
P.O. Box #061080
Wacker Drive Station - Sears Tower
Chicago, IL 60606-1080
Telephone 312/876-2606
Customer #26263
Attorneys for Appellants

CLAIMS APPENDIX

1. A method of managing software use by a software provider for distribution to a user, comprising the steps of:

storing inside the software predetermined first information;

providing the software to a software user on an information storage means prepared corresponding to the software and to be connected to an apparatus for running the software, which information storage means is capable of being accessed by the apparatus in a connected state;

encoding second information by using a first key of a key pair of an open key encoding format; and

transmitting the encoded second information to said software user for said software user to decode said transmitted encoded second information by using a second key of said key pair of said open key encoding format, and to read said first information from said information storage means, and to match said read first information against said decoded second information,

wherein said software is enabled when the information match, and

wherein the encoded second information is transmitted to the software user for matching the read first information against the decoded second information each time the software user uses said software.

2. A method of managing software use as set forth in Claim 1, further comprising the steps of:

receiving predetermined third information identifying the software provided along with said software and said information storage means from the user when said user seeks authorization of use of said software;

identifying said software user based on said transmitted third information; and

detecting second information to be matched against said first information stored in said information storage means given to the software user.

3. A method of managing software use as set forth in Claim 2, wherein said first information and said second information are selected from the group of information consisting of identification information for identifying said software user, identification information for

identifying said distributed software, and identification information for identifying said information storage means.

4. A method of managing software use as set forth in Claim 3, wherein said first and second information is a password added to said software and said information storage means.

7. A method of enabling software by a user for software managed by a software provider, comprising the steps of:

receiving software in an information storage means prepared corresponding to the software, predetermined first information being stored in the software;

connecting said information storage means with an apparatus for running the software, which information storage means is capable of being accessed by the apparatus in said connected state;

receiving encoded second information from said software provider to be matched against said first information stored in said information storage means, said encoding performed by using a first key of a key pair of an open key encoding format;

decoding said transmitted encoded second information by using a second key of said key pair of the open key encoding format;

reading said first information from said information storage means; and

matching said read first information against said decoded second information,

wherein said software is enabled when the information match, and

wherein the steps of receiving the encoded second information, decoding the transmitted encoded second information, reading the first information, and matching the read first information against the decoded second information are performed each time said software user uses the software.

8. A method of enabling software as set forth in Claim 7, further comprising the steps of:

transmitting predetermined third information identifying the software provided along with said software and said information storage means when seeking authorization of use of said software,

wherein said software provider identifies said software user based on said transmitted third information, and detects second information to be matched against said first information stored in said information storage means given to the software user.

9. A method of enabling software as set forth in Claim 8, wherein said first information and said second information are selected from the group of information consisting of identification information for identifying said software user, identification information for identifying said distributed software, and identification information for identifying said information storage means.

10. A method of enabling software as set forth in Claim 9, wherein said first and second information includes a password added to said software and said information storage means.

13. A system for enabling software stored in an information storage means for accessibly connecting via a predetermined interface means to an apparatus for running the software, said software having first information stored therein, comprising:

transmitting means for transmitting second identification information to a software provider when seeking authorization of use of said stored software;

receiving means for receiving encoded third information transmitted by said software provider to be matched against said first information generated based on said second information, said third information being encoded by a first key of a key pair of an open key encoding format;

decoding means for decoding said received encoded third information by using a second key of said key pair of the open key encoding format;

matching means for matching said first information stored in said information storage means against said decoded third information; and

execution control means for enabling said software to be used when the information match, and

wherein the encoded third information is received for matching against the first information each time a software user uses said software.

14. A system for managing software by a software provider, said software being stored in an information storage means to a provider for accessibly connecting via a

predetermined interface means to an apparatus for running the software, said software having first information stored therein, comprising:

receiving means for receiving second identification information from a user seeking authorization of use of said stored software;

encoding means for encoding third information by using a first key of a key pair of an open key encoding format based on said second information;

transmitting means for transmitting the encoded third information to said user to be matched against said first information,

wherein said first information stored in said information storage means is matched against said third information upon being decoded, and said software is enabled to be used when the information match, and

wherein the encoded third information is transmitted for matching against the first information each time the user uses said software.

EVIDENCE APPENDIX

Appellants do not submit extraneous evidence with this Main Brief on Appeal.

RELATED PROCEEDINGS APPENDIX

Appellants are not aware of any related appeals or interferences with regard to the present application.